Relevant Timeframe: From the release date until updated.

BLUF: Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) cyber actors are deploying a previously-undisclosed Linux malware called "Drovorub" against victims. NSA and FBI have partnered to release a joint advisory highlighting immediate actions stakeholders should take to protect against this threat.

- On 13 August, t**he National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) will publicly release an unclassified, dual-seal Cybersecurity Advisory (CSA) to publicly expose previously undisclosed Russian malware called "Drovorub."**

- Drovorub is a Linux malware toolset consisting of an implant coupled with a kernel module rootkit, a file transfer and port forwarding tool, and a command and control (C2) server. When deployed on a victim machine, Drovorub provides the capability for direct communications with actor-controlled C2 infrastructure; file download and upload capabilities; execution of arbitrary commands; port forwarding of network traffic to other hosts on the network; and implements hiding techniques to evade detection.

- The CSA will attribute the malware, to Russian cyber actors from the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), also known as Unit 26165, whose activity is sometimes identified by the private sector as APT 28, Fancy Bear, Strontium and a variety of other identities.

- The malware represents a threat because Linux systems are used pervasively throughout National Security Systems, Department of Defense, and the Defense Industrial Base. All stakeholders should take action as appropriate.

- **NSA and FBI are now sharing this information with customers and the public to ensure stakeholders can take action to mitigate this threat and to eradicate GTsSS reliance upon it. The detailed CSA will include detection techniques, related mitigations and configuration recommendations**

- **Detection techniques include methodologies and SNORT/Yara rules. Preventative mitigations include applying Linux updates and preventing untrusted kernel modules. Further information can be found in the CSA itself.**

- The exceptional partnership between **NSA and FBI was critical and by releasing this comprehensive guidance together, the capabilities of Russian military intelligence cyber actors will be countered and degraded.**

Note: **Please defer any media inquiries to MediaRelations@nsa.gov.**